Ekonomiczne Problemy Usług nr 2/2018 (131), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/2-14 | strony: 147–155

Jarosław Napiórkowski
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Systemów Informatycznych
jaroslaw.napiorkowski@wat.edu.pl

Sieciowy model systemu bezpieczeństwa informacji w administracji publicznej

Kody JEL: C02, C18, C69, D81, L32
Słowa kluczowe: administracja publiczna, model matematyczny, bezpieczeństwo informacji, zarządzanie ryzykiem
Streszczenie. Okresowe przeprowadzanie analizy ryzyka w jednostkach sektora finansów publicznych stało się wymogiem wraz z nowelizacją ustawy o finansach publicznych. Kolejnym z podstawowych wymagań, jakie stawiane są przed podmiotami realizującymi zadania publiczne, jest spełnienie zapisów Krajowych Ram Interoperacyjności. Przy okazji pojawia się wymóg okresowych analiz ryzyka. Niestety dość duży odsetek podmiotów publicznych w Polsce ma z tym problem. W niniejszym artykule autor prezentuje budowę sieciowego modelu systemu, którego zastosowanie upraszcza i automatyzuje proces analizy ryzyka.

Wprowadzenie

Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania organizacją. W jednostkach sektora finansów publicznych stało się ono wymogiem wraz z nowelizacją ustawy o finansach publicznych z 27 sierpnia 2009 roku (Ustawa, 2009). Kolejnym podstawowym wymaganiem, stawianym przed podmiotami realizującymi zadania publiczne, jest spełnienie zapisów Rozporządzenia Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności (Rozporządzenie, 2012), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – jednym z nich jest konieczność przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań

minimalizujących to ryzyko. Niestety, jak wynika z raportu Najwyższej Izby Kontroli (NIK, 2016), w ośmiu urzędach (tj. 33,3%) w okresie objętym kontrolą nie przeprowadzano audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Najczęstszym wytłumaczeniem tego jest brak kadry z niezbędną wiedzą z tego zakresu. Wynika to jednocześnie z tego, że analiza ryzyka jest skomplikowanym procesem mającym na celu zapewnienie optymalnego poziomu kosztów systemu bezpieczeństwa i stosowanych zabezpieczeń w stosunku do przewidywanego ryzyka. Problemem może być również samo podejście i narzędzia stosowane do prowadzenia procesu oceny ryzyka.

1. Normy dotyczące zarządzania ryzykiem

Międzynarodowa Organizacja Normalizacyjną (ISO – *International Organization for Standardization*) opracowała wiele norm określających standardy zarządzania ryzykiem, nazywane ogólnie rodziną norm ISO 31000. Jednym z dokumentów jest norma PN-ISO 31000:2012 zawierająca zasady i ogólne wytyczne dotyczące zarządzania ryzykiem w sposób systematyczny, przejrzysty i wiarygodny w dowolnym zakresie i kontekście. Kolejnym, ogólnie znanym i powszechnym opracowaniem opisującym koncepcję i proces oceny ryzyka jest norma PN-EN 31010:2010 (Zarządzanie ryzykiem – Techniki oceny ryzyka), która dostarcza wskazówek do wyboru i stosowania systematycznych i metodycznych technik oceny ryzyka. W normie opisano koncepcję i proces oceny ryzyka. Ocena ryzyka przeprowadzana zgodnie z tą normą wspiera inne działania zarządzania ryzykiem. Przedstawiono w niej także zastosowanie niektórych technik, odwołując się do innych norm międzynarodowych, opisujących bardziej szczegółowo koncepcję i zastosowanie technik, które w normie wskazane są jako np. burza mózgów (*brainstorming*), technika delficka, wstępna analiza zagrożeń, analiza rodzajów błędów oraz ich skutków – FMEA (*Failure Mode and Effects Analysis*), analiza drzewa błędów – FTA (*Fault Tree Analysis*) czy też metody bayesowskie.

Techniki klasyfikowane są według podziału pod kątem ich zastosowanie na etapie:

- identyfikacji ryzyka,
- analizy konsekwencji na etapie analizy ryzyka,
- jakościowego, ilościowego lub półilościowego oszacowania prawdopodobieństwa na etapie analizy ryzyka,
- oceny skuteczności istniejących kontroli na etapie analizy ryzyka,
- oszacowania poziomu ryzyka na etapie analizy ryzyka,
- ewaluacji ryzyka.

Na każdym z etapów oceny ryzyka możliwe jest stosowanie różnych narzędzi i metod. Zestawienie (*Table A.1 – Applicability of tools used for risk assessment*) zawiera klasyfikację, proponującą techniki jakie mogą być stosowane do każdego etapu oceny ryzyka i ich przydatność.

Metody oparte na statystyce bayesowskiej i sieciach Bayesa klasyfikowane są w niej jako nieznajdujące zastosowania przy identyfikacji ryzyka jakościowego, ilościowego lub

półilościowego oszacowania prawdopodobieństwa na etapie analiza ryzyka czy też oszacowania poziomu ryzyka na etapie analizy ryzyka. Jednocześnie norma wskazuje je jako zdecydowanie mające zastosowania przy analizie konsekwencji na etapie analizy ryzyka oraz ewaluacji ryzyka. Jednocześnie wskazywane są następujące ograniczenia:

- zdefiniowanie wszystkich zależności w sieci Bayesa może być niewykonalne ze względu na złożoność i wynikające z tego koszty,
- podejście bayesowskie wymaga znajomości wielu prawdopodobieństw warunkowych, które są na ogół określane na podstawie wiedzy eksperckiej, oprogramowanie oparte na sieci Bayesa może dostarczyć odpowiedzi tylko na podstawie takich założeń.

2. Model sieciowy

Zaletą modeli sieciowych jest przede wszystkim prostota ich interpretacji. Modele sieciowe przedstawione w postaci graficznej są zrozumiałe nie tylko dla osób zaangażowanych w ich tworzenie. W przypadku oceny ryzyka, niewątpliwą zaletą modelu sieciowego jest możliwość wizualizacji powiązań między skutkami zagrożeń. Problemem może być jednak sposób budowy takiego modelu sieciowego.

Zdecydowana większość stosowanych dziś metodyk analizy ryzyka, oparta jest wyłącznie na wiedzy eksperckiej osoby prowadzącej tę analizę. Stawianie tylko takiej gwarancji bezpieczeństwa w budowanym systemie może prowadzić do poważnych uchybień, wynikających z celowego lub przypadkowego pominięcia lub niedostrzeżenia zagrożenia. Równie niebezpieczne może być niedostrzeżenie podatności zasobu na określone zagrożenie. Oszacowanie ryzyka realizacji zagrożenia wobec zasobu jest całkowicie uzależnione od eksperckiej znajomości zagadnienia.

Wszystkie wymienione niedoskonałości metodyki analizy ryzyka mogą powodować nieszczelność systemu ochrony, co w efekcie może doprowadzić do utraty poufności, dostępności lub integralności chronionych informacji.

Proces analizy ryzyka wymaga na każdym etapie weryfikacji wyników przez innych ekspertów. Iteracyjność i złożoność tego procesu powoduje, że jest on długotrwały (przez to kosztowny), a jednocześnie nie ma gwarancji jego poprawności i kompletności. Metodykę budowy modelu sieciowego można zaprezentować w postaci modelu kontekstowego (Adamczyk, Kiryk, Napiórkowski, Walczak, 2016a):

Rysunek 1. Model referencyjny sieci

Źródło: Adamczyk i in. (2016a).

Podjęto próby automatyzacji budowy analizy ryzyka, które wykazały złożoność tego problemu, wskazując jednocześnie kluczową rolę eksperta. Jednocześnie szersze spojrzenie na uzyskane wyniki pozwoliło zauważyć następującą prawidłowość:

1. Zasoby opisywane są rzeczownikami,
2. Zagrożenia opisywane są rzeczownikami,
3. Podatności są opisywane przymiotnikami lub (w języku polskim) imiesłowem przymiotnikowym albo wyrażeniem przymiotnikowym.

W odniesieniu do modelu referencyjnego sieci otrzymujemy następujący kontekstowy (w sensie gramatyki) model sieci:

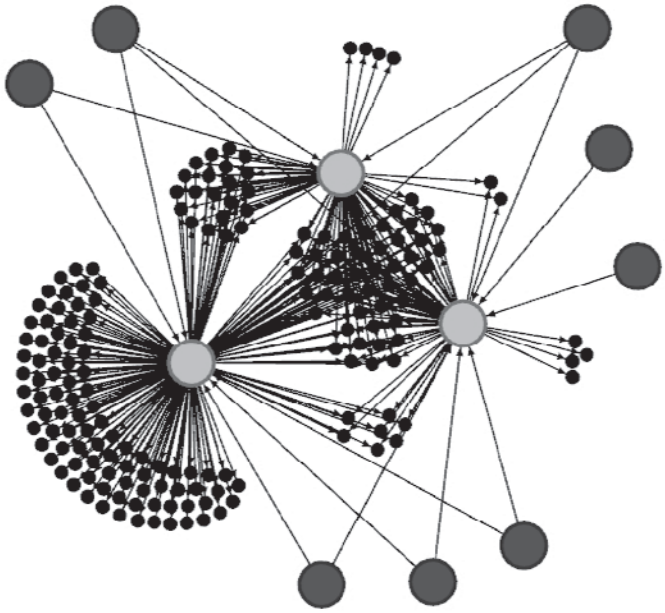
Rysunek 2. Model kontekstowy sieci

Źródło: Adamczyk i in. (2016a).

Adamczyk, Kiryk, Napiórkowski, Walczak (2016b) wykorzystując powyższy model, zaproponowali algorytm, który opisuje proces identyfikacji zasobów, podatności oraz zagrożeń w ujęciu kontekstowym. W algorytmie tym do utworzenia odpowiednich danych, służących do zbudowania grafu sieci z trójki kontekstowego modelu sieci, wykorzystano specjalnie opracowany algorytm oparty na systemach słownikowych. Algorytm ten zredukował jednocześnie złożoność problemu, eliminując z pełnego iloczynu kartezjańskiego wymienionych składowych te, które nie pozostają w żadnej relacji. Pozwoliło to na zbudowanie urealnionego modelu sieciowego, odpowiadającego rzeczywistości. Zatwierdzenie eksperckiego modelu jest podstawą do rozpoczęcia budowy modelu sieciowego, w którym węzłami są zasoby, zagrożenia i podatności. Dla budowy modelu sieciowego kluczowy jest efekt łączenia w trójki par zasób–podatność i zagrożenie–podatność za pośrednictwem relacji i powiązań wychodzących z węzłów obrazujących podatności, tak jak w schemacie na rysunku 2.

Przyjęty model kontekstowy powoduje, że finalnie można utrzymać akceptowalny poziom złożoności i spowodować budowanie relacji w sposób podlegający obiektywnej kontroli sterowanej regułą przedstawioną na rysunku 2.

W trakcie budowy modelu sieciowego skorzystano z tego, że każde zagrożenie oddziałuje na zasób wyłącznie przez podatność, którą ma ten zasób. Oznacza to, że zagrożenie może wpływać na zasób wyłącznie w kontekście występowania określonej podatności.

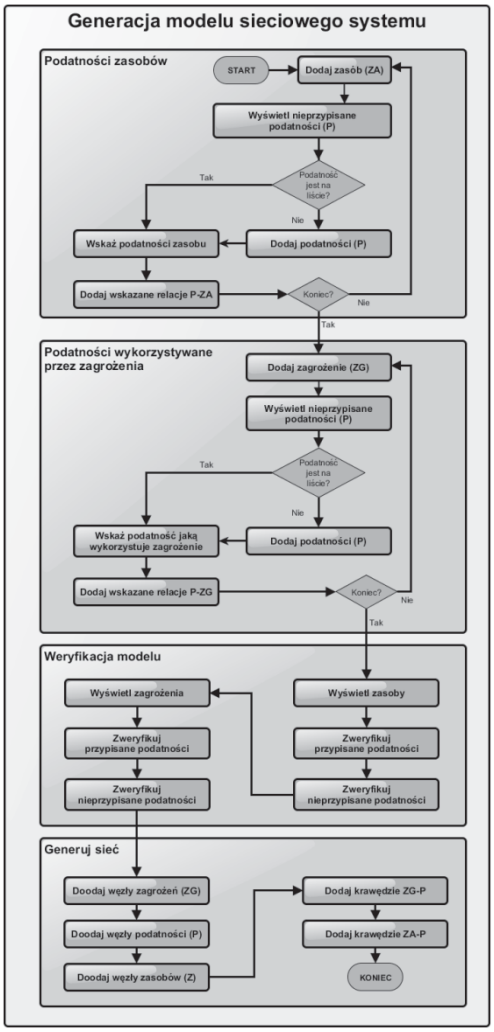


Rysunek 3. Graf sieci dla przykładowego modelu – wybrany fragment zasobów (kolor czarny – węzeł zasobu, kolor jasnoszary – węzeł podatności, kolor grafitowy – węzeł zagrożenia)

Źródło: Adamczyk i in. (2016a, 2016b).

Szczególnie ciekawym elementem modelu sieciowego jest możliwość wyliczenia charakterystyk, które jednoznacznie wskazują wpływ struktury sieci i poszczególnych jej węzłów na propagowanie zagrożenia w takiej strukturze.

Siła oddziaływania poszczególnych elementów sieci ma cechy zarówno lokalne, wynikające z bezpośredniego otoczenia badanego elementu, jak i cechy globalne (lub raczej nielokalne), wynikające ze specyfiki struktury sieci w szerszym otoczeniu badanego elementu. W strukturze sieci można wyznaczyć wartości liczbowe wybranych charakterystyk jej elementów (w szczególności węzłów sieci), które opisują siłę oddziaływania tych elementów w jej strukturze.



Rysunek 4. Schemat generacji modelu sieciowego

Źródło: Adamczyk i in. (2016b).

3. Miary centralności sieci

Rozważmy typowe charakterystyki wyliczane dla węzłów sieci, wprowadzając pojęcia miar centralności węzła, bliskości i pośrednictwa za pracą Borgatti, Everett, Freeman (2002). Podobne miary centralności wprowadzono przy analizie sieci złożonych (Bartosiak, Kasprzyk, Tarapata, 2011).

Miara centralności definiuje jak ważny w całej sieci jest węzeł. Miary centralności służą do zmierzenia intuicyjnego odczucia że w większości sieci rzeczywistych złożonych, niektóre wierzchołki lub krawędzie są bardziej ważne/prestiżowe od innych.

Określenie centralności w sieciach analizujących bezpieczeństwo pozwala wyłonić kluczowe podatności i zagrożenia. Centralność może dotyczyć węzłów i całej sieci.
Dla grafu nieskierowanego stopniem centralnym C_d jest:

$$C_d(v_i) = d_i$$

gdzie d_i oznacza stopień (liczba sąsiadujących krawędzi) węzła (v_i).
W przypadku grafów skierowanych wyróżniamy dwie odrębne miary stopnia centralności tzw. centralność wejściową (*indegree centrality*) oraz centralność wyjściową (*outdegree centrality*).

Prestiż i towarzyskość węzła to miara pokazująca, że węzeł jest bardziej istotny z uwagi na to, iż komunikuje się z większą liczbą innych węzłów a preferowane są węzły z większą liczbą krawędzi wychodzących, dzięki czemu określamy rozgłos węzła. Podczas korzystania z d_i^{in} wyliczamy jak popularny jest eksponowany węzeł, a jego wartość pokazuje znaczenie lub prestiż (*prominence or prestige node*). Podobne obliczenia należy wykonać aby obliczyć towarzyskość węzła d_i^{out} (*gregariousness node*).

Bliskością (*closeness, reach*) węzła nazywamy średnią długość najkrótszych ścieżek między danym węzłem i wszystkimi pozostałymi węzłami. Jest to zatem oczekiwana odległość między danym węzłem i dowolnym, innym węzłem.

Pośrednictwo (*betweenness)* to zdolność węzła w sieci do tworzenia połączeń między innymi węzłami. Węzeł o wyższej wartości tego parametru niż inne węzły w sieci nazywamy często hubem.

W naszej sieci jeśli węzeł podatności ma wysoki stopień, czyli łączy wiele węzłów zasobów z dużą liczbą węzłów zagrożeń, to jednocześnie będzie miał bliskość (*reach*) także wysoką, bo duża liczba węzłów może go osiągnąć w jednym kroku w sieci. Pośrednictwo natomiast będzie dla każdego węzła podatności zależeć praktycznie tylko od struktury sieci. Im bliższa jedynki będzie wartość pośrednictwa dla węzła o jednocześnie wysokim stopniu, tym taka podatność w strukturze analizy ryzyka będzie węzłem bardzo istotnym, o dużej sile oddziaływania.

Prawdopodobieństwo wystąpienia zagrożenia $p(zag)$ zwykle wyznaczamy na podstawie wiedzy eksperckiej o właściwościach zagrożeń. Jednak to, czy i w jakim stopniu wystąpienie zagrożenia oznaczać będzie wystąpienie ryzyka na konkretnym zasobie zależy od struktury sieci, a w szczególności od ulokowania w niej węzłów podatności zasobu na zagrożenie. Pierwszym przybliżeniem będzie zależność funkcji zagrożenie zasobu $F(z)$ od struktury podatności badanego zasobu. Przy pewnym prawdopodobieństwie zagrożenia $p(zag)$ jego oddziaływanie na zasób może być opisane jako:

$$F(z) = B \bullet p(zag)$$

Gdzie B jest wartością wyliczoną pośrednictwa podatności w badanej sieci dla węzła podatności przekazującego zagrożenie do zasobu. Ten zapis nie budzi wątpliwości kiedy istnieje pojedynczy węzeł podatności pomiędzy grupą zasobu, a węzłem zagrożenia.

Podsumowanie

W artykule do przeprowadzenia analizy ryzyka zaproponowano mieszany, ekspercko-formalny model analizowania ryzyka zagrożenia zasobu. Składnik ekspercki modelu obecny jest zawsze na etapie tworzenia trójki „zasób – podatność – zagrożenie". Wynika on z metodyki budowania modelu sieciowego i zasad analizy ryzyka. Uzyskuje się dzięki temu matematyczny model sieciowy o budowie typowej dla sieci złożonych, w którym wprowadzono nowe pojęcie funkcji zagrożenia zasobu, co zależy od struktury sieci. Widzimy także, że przyjęta metodyka w zadaniu analizy ryzyka wyznacza nam strukturę sieci. Wartość liczbową ryzyka obliczamy przy zadanych prawdopodobieństwach wystąpienia zagrożeń i skutkach na zasobie wyznaczonych przez opis ekspercki, ale wykazujemy (czego nie da się zrobić bez modelu sieciowego) jak zależy ona od matematycznego modelu struktury sieci.

Systematyczne, zgodne z zaproponowanym schematem generacji modelu sieciowego podejście do budowy modelu analizowanego obszaru pozwala na relatywnie łatwe przygotowanie modelu sieciowego systemu. Możliwość przedstawienia modelu w postaci graficznej czyni zbudowany model zrozumiałym nie tylko dla osób zaangażowanych w ich tworzenie. To zaś pozwala na jego szerokie i łatwe stosowanie podczas analizowania ryzyka. Analiza ryzyka oparta na statycznych charakterystykach sieci pozwala na szybkie, wiarygodne i uniezależnione od subiektywnych odczuć zbieranie charakterystyki analizowanego obszaru a dzięki temu szybkie wskazywanie aktywów w organizacji, które są narażone na wysokie prawdopodobieństwo zmaterializowania się zagrożenia. Opisany schemat budowy modelu sieciowego pozwala na prowadzenie analizy ryzyka po każdej zmianie, która może wpływać na funkcjonujący system zarządzania bezpieczeństwem informacji.

Bibliografia

Adamczyk, P., Kiryk, G., Napiórkowski, J., Walczak, A. (2016a). Sieciowy model systemu bezpieczeństwa. W: Kiedrowicz M. (red.), *Zarządzanie informacjami wrażliwymi. Bezpieczeństwo dokumentów, wykorzystanie technologii RFID*. Warszawa: Wojskowa Akademia Techniczna.

Adamczyk, P., Kiryk, G., Napiórkowski, J., Walczak, A. (2016b). *Network model of security system*. MATEC Web of Conferences 76, 02002.

Bartosiak, C., Kasprzyk, R., Tarapata, Z. (2011). Application of Graphs and Networks Similarity Measures for Analyzing Complex Networks. *Biuletyn Instytutu Systemów Informatycznych*, *7*, 1–7.

Borgatti, S.P., Everett, M.G., Freeman, L.C. (2002). *Ucinet 6.0 for Windows: Software for Social Network Analysis*. Harvard: Analytic Technologies.

Raport NIK (2016). *Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego*. Pobrane z: https://www.nik.gov.pl/plik/id,10420,vp,12749.pdf.

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012, poz. 526.

Ustawa z 27 sierpnia 2009 roku o finansach publicznych, Dz.U. 2009, nr 157, poz. 1240.

NETWORK MODEL OF INFORMATION SECURITY SYSTEMS OF PUBLIC ADMINISTRATION UNIT

Keywords: public administration, mathematical model, information security, risk management

Summary. Periodic risk analysis in units of the public finance sector has become a requirement along with the amendment to the Public Finance Act. However, a large percentage of public entities in Poland has a problem with this. The article presents the concept of building a network security model and its application in the process of risk analysis. It indicates the possibility of a new definition of the role of the network models in the safety analysis. Special attention was paid to the development of the use of an algorithm describing the process of identifying the assets, vulnerability and threats in a given context.

Translated by Jarosław Napiórkowski

Cytowanie

Napiórkowski, J. (2018). Sieciowy model systemu bezpieczeństwa informacji w administracji publicznej. *Ekonomiczne Problemy Usług*, *2* (131/2), 147–155. DOI: 10.18276/epu.2018.131/2-14.